开篇词 | 别说你没被安全困扰过

2019-12-09 何为舟

安全攻防技能30讲 进入课程 >

讲述：何为舟

时长 09:32 大小 8.74M

你好，我是何为舟，很高兴能在这里和你聊安全。

我喜欢安全，本科和硕士读的都是信息安全专业。在工作中，我会把自己想象为一名仗剑走天涯的侠客，哪里有安全问题，我便会拔刀相助。我喜欢那种解决完问题后的快感，那场景就好像有人和我说，“感谢大侠的救命之恩”。

我现在是美团点评的安全平台负责人。在加入美团之前，我曾任职于新浪微博，负责网络安全和业务安全方向的整体研发和设计工作，这其中包括攻防对抗、安全工具开发、风控系统等。

作为一个安全侠客，我打过全球流行的网络安全竞赛CTF，做过渗透测试，还考取了信息系统安全专业认证。在安全这件事情上，我还真有挺多话题想和你聊。

为什么要学安全？

首先，不知道你是否还记得 2017 年 9 月美国知名征信公司 Equifax 的数据泄露事件，这事导致了 1.45 亿美国居民个人隐私信息被泄露。受事件影响，Equifax 公司市值瞬间就蒸发了 30 亿美元，最后还赔偿给用户 4.25 亿美元，可谓损失惨重。后来，Equifax 公司复盘了安全事故的原因，发现这个事故的罪魁祸首，居然是一个早已被披露出来的安全漏洞，叫作 Apache Struts，真是让人哭笑不得。

你说这事难吗？现在看起来，一点都不难。但问题出现在什么地方呢？我觉得核心点是 Equifax 公司的工程师可能没有安全意识，也没有把安全当成一个优先级很高的事情去做。

同样的事情其实还有很多，我觉得 Equifax 公司的低级安全事件，应该给我们每一个程序员敲响警钟，**我们在追求开发效率的同时，一定要把“安全”这俩字“放在心上”。**

其次，从公司的角度来说，安全同样是不可或缺的一环。

任何一家公司都会存在安全的刚需问题，肯定需要有人来解决它。但是，公司招人组建安全团队，需要投入较大的成本。而这部分安全的成本，很多时候并不产生直接的收益。因此，对很多公司来说，业务都没成熟，就去考虑安全，是不合算的。这也就产生了一种现状：**小公司没有安全，大公司都在“补”安全。**

从安全发展角度上来讲，这种前期不重视安全，后期再补安全的做法，是很不利的。一方面，在发展前期留下了极大的安全隐患，公司可能在一次攻击后就彻底垮台了。另一方面，后期补安全，会因为安全去改动已经发展成熟的业务，导致安全和业务产生冲突，从而阻碍安全发展。

于是，矛盾点就产生了：很多规模不大的公司不愿意投入成本去做安全，但从长远考虑又需要安全。那该怎么办呢？我认为，**如果业务的开发和管理人员，能够具备基础的安全知识，尽早做好安全规划，就能够以很低的成本满足公司前期的安全诉求。**

因此，如果你想要在企业的全面发展中占据一席之地，或者是在管理方向上走得更“远”，那么我建议你，尽早地掌握安全知识，掌握企业安全防护的专业技巧。

我们究竟该怎么学习安全呢？

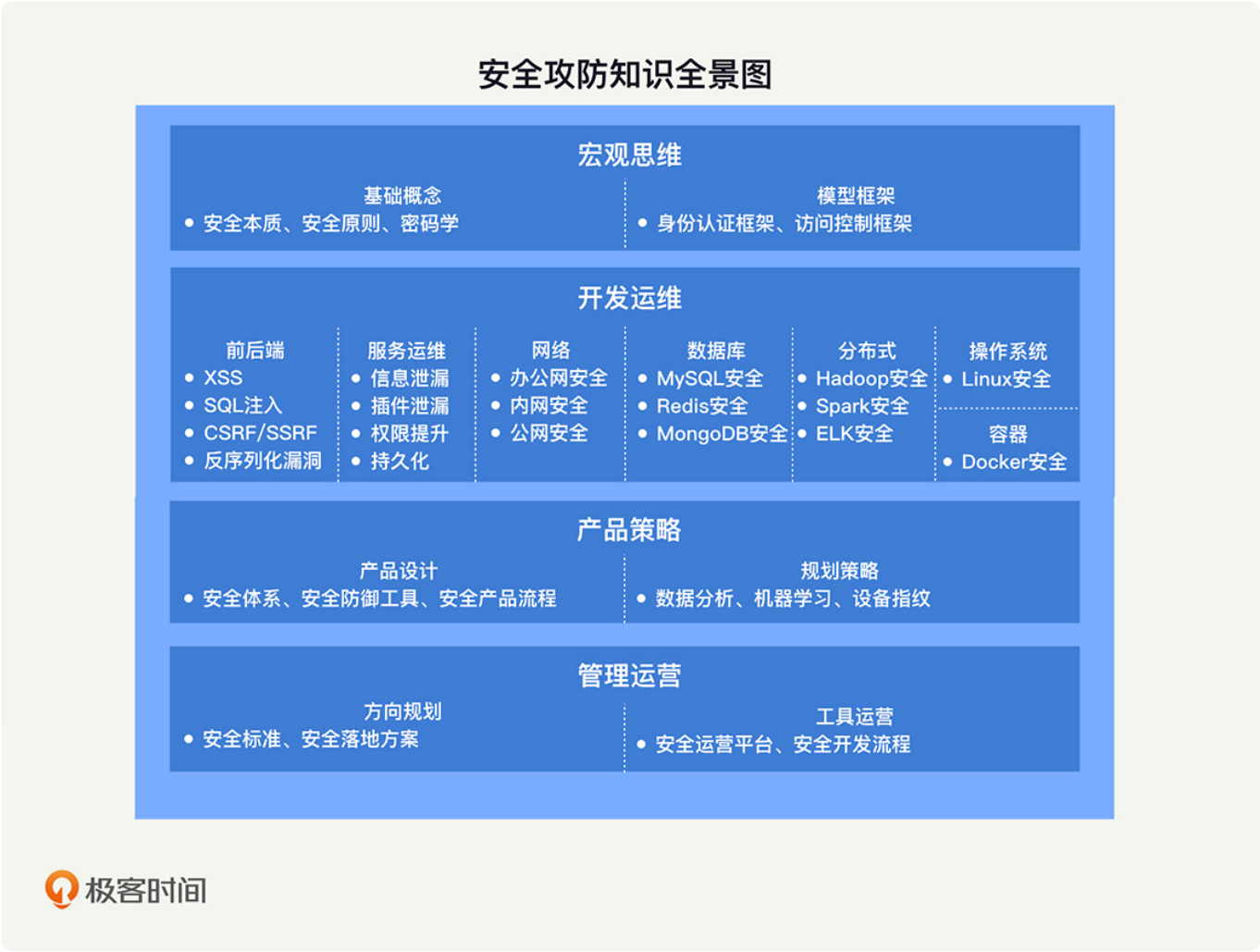
你可能会存在这样的顾虑：安全可能需要花上几年时间学习和实践才能小有所成，时间成本是否有点高呢？确实，想要真正做好安全，时间的磨砺是不可或缺的。但是，这并不意味着你需要几年后再去从事安全相关的工作。正如上面所说的，公司初期的安全需求相对简单。因此，你完全可以快速入门，然后投入到公司的安全需求中去。接下来，**你就可以随着公司的发展，边学习边做安全**。

那么，学习安全是否门槛很高、难度很深呢？学习安全的过程中，你可能需要懂前端、懂后端、懂操作系统、懂网络。需要懂的知识非常多，但幸运的是，对于安全入门来说，宽度比深度更重要。因此，对于这些基础知识，深刻理解自然更好，但是懂些皮毛也足够了。在专栏中，我也会由浅入深，对安全需要的基础知识进行讲解。

你还可能会问：没有实践的机会，我能不能学好安全呢？确实，实践出真知，个人安全能力的提升，需要经过不断地磨练。跟着专栏进行学习，我相信你可以具备解决安全问题的基本能力。为了帮助你快速实践，我会通过思考题的形式，去引导你分析自己所在公司的现状和未来。你可以将你的所思所想发表出来，共同探讨，进行“沙盘演练”。

总结来说，本次专栏的定位是**安全基础课**。在专栏的覆盖面上，我会力求全面，让你能够了解安全的方方面面。我希望，通过对安全专栏的学习，你能够具备安全思维，在遇到安全问题的时候，有解决问题的方向和路径。

这里，我为你准备了一张安全攻防知识全景图，包含你需要掌握的所有相关知识。建议你最好保存下来，在之后的学习过程中，有针对性地去训练自己。



在内容设计上，我根据安全方向的不同，把专栏内容划分为五个模块。

在第一模块“安全基础”中，我首先会为你系统地讲解安全基础概念、思考框架，以及解决安全问题的思路，带你从理论层次认知安全，让你能够系统地看待安全问题、评估安全需求，为你的安全学习指明方向。

在第二模块“Web 安全”中，我会为你讲述 Web 安全中一些经典安全问题的成因，结合当下 App 端各类接口中存在的 Web 漏洞，让你了解常见的 Web 攻防手段，帮助你在开发时，从源头切断安全问题。

在第三模块“Linux 系统和应用安全”中，我会为你讲解底层攻击的各种手段，以及它们会产生的影响，让你掌握其中的原理，能够在部署底层设施时，遵守安全事项，避免产生运维层面的安全问题。

在第四模块“安全防御工具”中，我会结合真实的安全防护案例，为你介绍六大安全防御工具的使用方法和适用场景。另外，我还会总结一些常见的安全防御手段，引导你建设系统级

的安全防御体系。

在第五模块“业务安全”中，我会为你讲解“黑灰产”的常见手段，教你识别查找“黑灰产”的方法及防护策略。另外，我还会联系实际业务场景，手把手教你系统解决业务安全问题。

我希望学完这个专栏之后，你能够**既懂“攻”又懂“防”，既懂理论也懂实践**。比如，你既能知道怎么发起一个简单的 SQL 注入攻击，也能够知道怎么从代码开发层次进行防御，同时也会了解到怎么通过和代码接耦合的 WAF 去做防御。又比如，你会知道怎么去规划和设计安全体系，以及在不同的阶段应该做什么事。

除了正文之外，我还设计了几篇不定期加餐，来和你聊一聊目前一些热门的安全方向，希望能够加深你对安全的理解。同时，加餐中也包含了我对个人发展的一些思考和建议。目前，安全行业普遍存在人才供给不足的现象，很多岗位招不到合适的人。因此，我希望结合我的个人经验，能够给想往安全专业发展的同学一些指引，教你成为“合适的人”。

最后，我想说，安全是一个特别重实践的领域，如果你有时间，一定要多练习，多总结。在课程设计中，我在每一节课后都留了思考题，希望你能够结合知识点，给出自己的思考。很多事情都没有标准答案，你梳理的过程本身也就是强化思考的过程，所以，千万不要有心理负担，大胆表达就可以了，我一定会尽我所能及时给你反馈。

如一开始所说，我喜欢安全，喜欢侠客精神。正在看这篇文章的你，我相信你也是如此。希望在接下来 3 个月的“刀光剑影”里，我们能互相切磋，一起成长！

© 版权归极客邦科技所有，未经许可不得传播售卖。 页面已增加防盗追踪，如有侵权极客邦将依法追究其法律责任。

下一篇　01 | 安全的本质：数据被窃取后，你能意识到问题来源吗?

精选留言 (28)

写留言

西西弗与卡夫卡
2019-12-09

行走江湖，安全第一

展开

8

业余草
2019-12-10

安全到底有多重要，我的服务器已经被植入了挖矿代码，还有很多发生了比特币勒索！https://mp.weixin.qq.com/s/hAQdUP0CtdHii9nyVT7w7A

展开

作者回复: 看这分析过程，大佬呀。

5

一步
2019-12-09

道路千万条，安全第一条

展开

3

瑞泉
2019-12-10

我做信息安全管理软件，安全事件分析一直困扰着我，如何制定规则，规则有哪些分类，等保2.0是分为审计类和安全类，哪些属于审计，哪些属于安全，又都有哪些规则？这些规则又如何才能有效果，望老师能给我解惑，十分感谢！

展开

> 作者回复: 等保会讲一讲我的理解。不过我司之前只过了2级，感觉比较水，干货不多。更多的是想讲讲如何去做好安全防御。

2

1

等一分钟
2019-12-09

希望和各位一起学安全，打开思路，理清思绪，开拓视野。另外需要提前了解些什么。

> 作者回复: 需要了解的太多，所以就不需要提前了解什么了。跟着课程边学边了解就好了，有不懂的就留言，或者自己百度，都行。

1

Chocolate
2019-12-09

被白帽子拿了好多钱，过来补一补

展开

> 作者回复: 哈哈，我们一个严重漏洞都是几万十几万的给

1

早起不吃虫
2019-12-09

听老师开篇词就目的明确踏实，先订阅一波

展开

1

二马

2019-12-15

企业信息安全由安全技术架构、安全流程制度和安全人员（意识）组成，相辅相成，光买产品堆砌无法达到很好的安全防护效果，因为安全在于建设更在于运营。运营既有技术层面的分析处置，也有流程制度方面的检查和规范。总的来说靠技术实现安全太难，从意识源头开始会事倍功半，如普通员工的安全意识，系统管理员的安全意识，开发人员的安全意识。当安全人人有责的意识深入人心，再辅以技术（安全产品，安全技巧），大部分...

展开

作者回复: 这么专业的评论，是同行嘛~

旺旺

2019-12-14

安全确实很重要，打卡了。期待老师的课程。

展开

进财

2019-12-13

网络安全的人力资源投入，资源投入，需要取得老板的认可还是比较困难的，有没有什么办法给老板洗脑，增加网络安全防护意识。

展开

作者回复: 你好，感谢你的留言。向上教育这个问题我相信很多人都有困惑，不过做法因领导而异，没什么统一的做法。就我之前的经验而言，最有效的办法是，挨了打就知道疼了。被入侵过，被薅几把羊毛，领导就开始重视了。即使你目前没人搞你，我觉得也可以在允许范围内，做一次演练，把问题暴露出来，推动起来会好做一些。

小风嗖嗖嗖

2019-12-11

看到广告 就买了，漂亮的课程。

展开

wong
2019-12-10

学完能找到工作嘛

展开

作者回复: 希望能

积极找工作
2019-12-10

课堂笔记：01风控与业务是矛盾的；02企业搞安全防止黑天鹅事件；03安全需要广泛的知识。

张诚
2019-12-10

开始安全之旅

展开

Middleware
2019-12-10

互相切磋、一起成长

展开

Ops360
2019-12-10

看到安全专栏，这就是我一直想需要的。经历了区块链挖矿，DDOS攻击，cc攻击，但还是不懂什么是安全，只是一味买买买一些防护产品。通过这个专栏的学习，我想真正懂得安全，感谢！

作者回复: 你好，感谢你的回复。确实我也发现很多公司其实有遇到问题，但不知道如何去解决。防护产品确实有它的价值，但如果不配合公司自身安全体系的建设，是没办法达到很高的安全水平的。所以，别被乙方忽悠啦～

闪耀之作
2019-12-10

kail安全渗透Web白帽子高级工程师我想做这个应该怎么学呢？在零基础的小白的前提下，前后端的技术如何跟安全渗透的技术进行联系学习呢？先后顺序不知道怎么样

作者回复: 首先，安全渗透不是本专栏的主要内容。如果从零入手的话，通常都是从web安全进行入手的，学习漏洞的过程中，自然会涉及到前后端的知识需要了解。这一块熟悉之后，就可以慢慢去了解一些系统应用的漏洞利用了。

攻城狮Ra
2019-12-10

安全攻防跟常说的挂外挂、Sql注入是不是有关，使用Hook对软件进行二次开发是否合法

作者回复: 有关，但不只是这些。
严格意义上说，不合法，我们之前抓过干这些的人。不过计算机犯罪的特殊性，举证过程，确实比较痛苦。

1

云轩
2019-12-10

公司天天收到上级信安部门的应用安全风险通报，每次看到“xxx系统存在安全风险，请马上关停整顿”都提心吊胆，晚上睡不着觉，按通报整改完了，还不知道是否还存在未知漏洞？自己很想体系化地去补一下安全这块的短板，看到这个课程毫不犹豫地报名了。

展开

作者回复: 现在很多公司都被入驻了网安办公室。。

niuniu
2019-12-10

CTF上遇到李现没，哈哈哈。

展开

作者回复: 李现打的是cs，不是ctf。估计为了过审，强行改成ctf了。。。